3 2 Fraud

Next, the question is addressed whether virus and hacking instances constitute fraud in terms of the South African common law.

3 2 1 General elements

Fraud can be defined as the unlawful and intentional misrepresentation that causes actual prejudice, or is potentially prejudicial, to another.[1] Therefore the elements of this offence are:[2] (a) Misrepresentation of an existing fact;[3] (b) actual or potential prejudice/harm; (c) unlawfulness; and (d) intent.

With regard to causation, the general opinion seems to be that because prejudice is so widely interpreted (potential prejudice will suffice), the causation requisite serves no purpose anymore:[4] It is no longer required that the deception has to be successful. The sole requirement is that the deception must be of such a nature that it is potentially prejudicial,[5] and therefore the court will hold that the accused committed fraud where there was actual prejudice which was not proved to be induced by the misrepresentation, provided the misrepresentation was potentially prejudicial.[6]

The intention element refers to two aspects, namely (a) the accused must firstly know or suspect that his (tacit or implied) representation or statement is false and (b) he must intend to defraud the complainant. The "intent to defraud" entails that a mere intention to deceive someone does not suffice; an intention to cause someone prejudice is required. Generally speaking, this means that A must induce B to embark on a course of action prejudicial to himself as a result of the misrepresentation.[7] Therefore the intent to defraud includes an intent to prejudice.[8] In *R v De Vos*[9] the court approved the following explanation of "intent to

---

* See 2004 *THRHR* 22 for part 1.

1 *S v Isaacs* 1968 2 SA 187 (D) 191C; *R v Henkes* 1941 AD 143 161.

2 See Snyman *Strafreg* (1999) 538; Joubert 6 *LAWSA* First re-issue (1996) para 328.

3 See *Isaacs* 191C–D.

4 See Snyman 541 and *LAWSA* para 323. For a contrary view see *Isaacs* 192A where the court stated that "[t]here must be a causal connection between the misrepresentation and the prejudice, whether the prejudice be actual or potential".

5 *R v Kruse* 1946 AD 524 533 534.

6 *Ibid.*

7 *R v Jones* 1926 AD 350 352.

8 *LAWSA* para 330.

9 1958 EDC 145.

defraud": "[W]ith intent to deceive in such a manner as to expose any person to loss or risk of loss."[10] It should also be kept in mind that the accused's motive is irrelevant and that no intention to acquire some advantage is required.[11]

Next, it must be ascertained what prejudice entails. All South African courts have maintained that the prejudice element does not necessarily refer to financial or proprietary damages.[12] Our courts have interpreted "prejudice" very widely and consequently it includes a vast spectrum of prejudicial facets (*benadelingsfasette*). South African courts have indicated that the following constitutes potential prejudice:

(1) Where the accused's conduct constitutes a risk of prosecution for the complainant or that the latter may lose his license (for instance to sell liquor).[13]

(2) Where the accused's conduct constitutes a risk of dishonour or loss of reputation to the complainant.[14] In *R v Dlamini*[15] the court maintained that a court must take

> "the widest view . . . of what prejudice means. It includes impairment of reputation or personal dignity . . . and we have assumed that the term is wide enough to cover any substantial inconvenience which the perpetration of the forgery may cause . . . The question is not what the forger obtains, but what the effect, or the potential effect, is upon some person other than the forger".[16]

Various other courts, including the Appellate Division, have also stated that "potential prejudice to one's honour or to one's reputation" is sufficient.[17]

(3) Where the accused's conduct constitutes a risk that the state may, for example, lose control over petrol consumption and/or liquor consumption and/or drivers of motor vehicles and/or foreign exchange.[18]

(4) Where the accused's conduct infringes third parties' rights. The following two cases illustrate this aspect: In *S v Myeza* the court noted:

> "Die nadeel hoef nie noodwendig die persoon teenoor wie die wanvoorstelling gemaak is te tref nie . . . [nadeel] sluit ook in die risiko van nadeel vir die Staat, plaaslike gemeenskappe, publiek *en derde persone in die uitoefening van hulle regte en die nakoming van hulle verpligtinge*."[19]

In *R v Jones* the court maintained that prejudice "include[s] any invasion of his civil rights".[20]

(5) Where the accused's conduct affects the complainant's state of mind. In *S v Harper*[21] the court maintained that

---

10 150.
11 *S v Shepard* 1967 4 SA 170 (W) 179D; *S v Van Biljon* 1965 3 SA 314 (T) 318.
12 *S v Myeza* 1985 4 SA 30 (T) 32C; *S v Kruger* 1961 4 SA 816 (A) 828B; *R v Dhlamini* 1943 TPD 20 23.
13 *R v Seabe* 1927 AD 28 33–34; *De Vos* 149 150.
14 *R v Seabe* 33.
15 1943 TPD 20.
16 23.
17 *R v Macatlane* 1929 TPD 708 712. See also *S v Rexsel* 1968 4 224 (A) 232F–G; *R v Heyne* 1956 3 SA 604 (A) 624H; *R v Jolosa* 1903 TPD 694 698.
18 *S v African Bank of South Africa Ltd* 1990 2 SACR 585 (W) 647e–f; *R v Jass* 1965 3 SA 248 (E) 250F–G; *R v Thebeta* 1948 3 SA 218 (T) 222.
19 32C. My emphasis.
20 352.
21 1981 2 SA 638 (D).

(b) he infringes the computer user's common law as well as constitutional right to privacy;

(c) the computer user loses control (even if only for a few seconds) over the digital content stored on his hard drive;

(d) should third parties learn that the computer user's system was penetrated, such conduct might lead to an infringement of *fama* and/or goodwill.

6.3 NB

3 2 2 3 The element of "intent to defraud" (E)

As noted earlier, the accused (the hacker) must have the intent not only to deceive the computer user, but also to prejudice him. It is submitted that since the mere intrusion of a computer constitutes potential prejudice to the computer user, and seeing that the accused is aware that by means of his unlawful conduct he infringes upon the computer user's civil rights (the right to privacy, the right of control over the digital content stored on his hard drive, the right to control access to such digital content and possibly his right to immaterial property), he has the necessary intent to prejudice.

7.1 NB

An example of another type of fraud by means of the Internet is found in the US case of *Hotmail Corporation v Van Money Pie Inc et al*.[42] The defendants sent spam (unsolicited commercial e-mail) to the e-mail accounts of other Hotmail subscribers. The defendants altered (spoofed) the return addresses of their e-mails to falsely indicate that they were sent from a Hotmail account, rather than from their true source. The plaintiff (Hotmail) applied for an interdict prohibiting the defendants from sending spam, indicating that these messages came from them (Hotmail). The court held that the defendant's conduct constituted fraud:

> "[D]efendants fraudulently obtained a number of Hotmail accounts, promising to abide by the Terms of Service without any intention of doing so and suppressing the fact that such accounts were created for the purpose of facilitating a spamming operation, and that defendants' fraud and misrepresentation caused Hotmail to allow defendants to create and use Hotmail's accounts to Hotmail's injury. In addition, the evidence supports a finding that defendants' falsification of e-mails to make it appear that such messages and the responses thereto were authorized to be transmitted via Hotmail's computers and stored on Hotmail's computer system – when defendants knew that sending spam was unauthorized by Hotmail – constitutes fraud and misrepresentation, and that Hotmail relied on such misrepresentations to allow the e-mails to be transmitted over Hotmail's services and to take up storage space on Hotmail's computers, to Hotmail's injury."[43]

7.2

It is submitted that address spoofing can also be prosecuted under South African criminal law as fraud.

NB

3 2 2 4 Must a system administrator be deceived?

In the previous paragraphs it was stated that the hacker misrepresents to the system administrator that he is an authorised user of the system. The question under this heading is: Who does the hacker deceive, if there is no system administrator, for instance, where he penetrates the security system of a normal (home) computer?

7.3

---

42 47 USPQ 2d 1020 (ND Cal 1998).
43 1025 para 37.

It is submitted that under such circumstances the hacker misrepresents to the computer owner (or any person in control of the computer at that particular moment) that he is either the "operating system" of the user's computer, when he views, copies, modifies or deletes files, or that he has authorised access to that particular computer (such as the user's Internet Service Provider). Even if this submission is incorrect, the prosecution is assisted by section 103 of the Criminal Procedure Act[44] which provides that

> "[i]n any charge in which it is necessary to allege that the accused performed an act with an intent to defraud, it shall be sufficient to allege and to prove that the accused performed the act with intent to defraud *without alleging and proving* that it was the intention of the accused *to defraud any particular person*, and such a charge need not mention the owner of any property involved *or set forth the details of any deceit*".[45]

The prosecution is, therefore, not required to stipulate or prove that the hacker intended to defraud a particular person. Furthermore, the prosecution is not obliged to stipulate who the owner of the computer system is.

3 2 2 5 Is the breaking or penetrating of security measures a requirement?

When fraud was discussed in the context of making misrepresentations to the system administrator or a person in control of the computer, the example used was where the hacker penetrated the computer's security measures or used someone else's password and username. A further question to be addressed here is: Whenever a particular computer system does not have security measures employing passwords and/or usernames, does the hacker make a misrepresentation that he is an authorised user or that he has authorised access? Many home computers, connected to the Internet, have no security measures installed to protect the computer from hacking and/or virus instances.

As noted above, in *S v Mbokazi*[46] an employee withdrew funds by means of a computer. The court maintained that the accused (as an employee) *impliedly* represented to the bank (his employer) that the client had duly authorised the transaction.

The fact that the computer in question lacks security measures, providing protection against hackers, should make no difference: The hacker still makes the implied misrepresentation that he enjoys the authorisation of the computer owner to *use* the computer. Whenever a hacker gains access to a computer and either merely observes the content (by clicking on files and documents) or deletes or copies such files, he *uses* the computer.

3 2 2 6 Does an unsuccessful attempt to hack constitute fraud or attempted fraud?

The question in this context is: When a hacker attempts to hack into another person's computer but fails to succeed, does he commit fraud or attempted fraud?

It was concluded above that a hacker makes a misrepresentation that he is an authorised user of the computer system, or that he has authorised access to that particular computer, and that such conduct is unlawful. Therefore, only two elements of fraud, namely intent and (potential) prejudice, still need to be addressed here.

---

44 Act 51 of 1977.
45 My emphasis.
46 *Supra* fn 38.

With regard to intent, it was observed above that the mere intent to mislead the complainant does not suffice. The law requires intent to cause prejudice to the complainant. South African courts have also noted that for conduct to constitute fraud, it is not required that the complainant should have believed the accused (the hacker).[47] The question of law that arises is: Whenever a hacker attempts to penetrate a computer system but fails, is intent to defraud the complainant present?

It is submitted that where a hacker attempts to penetrate a computer system, he poses the following risks:

(a) A risk that the owner may lose control over his computer, if the hacker (for instance) renders the owner's hard drive inaccessible or inoperable.

(b) A risk that the owner may lose control, temporarily or permanently, over his digital files, if the hacker deletes, modifies, copies or views them.

(c) A risk of infringing the owner's immaterial property rights (such as copyright, right to confidential information, right to goodwill and right to trade without unlawful interference), should the hacker succeed in penetrating the security system.

(d) A substantial risk of infringing the owner's common law, as well as constitutional, right to privacy.

(e) A risk of loss of reputation should third parties such as clients or potential clients discover or learn that a hacker penetrated the business' computer system. There is also the risk of negative media publicity.

(f) A risk of loss of credibility in the computer system: Employees may be reluctant to store confidential information on the hard drive for fear that the hacker may have installed an undetectable Trojan horse that will forward to its creator sensitive business information, as well as inform him of the passwords that render access to the computer system.

Therefore, it is submitted that the element of potential prejudice is present: A risk of prejudice existed when the misrepresentation was made.[48] It is further submitted that such "potential prejudice" is not too remote in that some local courts were willing to recognise a risk of loss of reputation where the complainant was defrauded by the accused.

It is also contended here that there is authority for the submission that an unsuccessful hacking attempt constitutes potential prejudice. Snyman gives the following example of fraud:

> "Veronderstel X verseker alle items wat aan hom behoort by 'n sekere versekeringsmaatskappy teen diefstal. Daarna eis hy 'n bedrag geld van die versekeringsmaatskappy op grond daarvan dat sekere artikels wat aan hom behoort, gesteel is ... Veronderstel egter dat, nadat X sy eis ingedien het, die versekeringsmaatskappy uitvind dat die tersaaklike items nie gesteel is nie en dat X se eis dus op 'n valse bewering gegrond is. Die maatskappy weier gevolglik om die bedrag geëis aan hom uit te betaal. Kan X nietemin nog aan bedrog skuldig bevind word? Die antwoord op hierdie vraag is bevestigend, omdat, alhoewel die maatskappy geen daadwerklike nadeel gely het nie, X se wanvoorstelling *potensiële* nadeel ingehou het."[49]

47 See eg *S v Swarts* 1961 4 SA 589 (E) 591D–E.
48 See *S v Campbell* 1991 1 SACR 503 (Nm) 508h–i; *Kruger* 828A; *R v Deale* 1960 3 SA 846 (T) 848A–B.
49 Snyman 538.

This argument is supported by South African judgments. In *Moolchund v R*[50] the accused fraudulently claimed compensation from the government. However, the latter discovered this and refused to pay. The court found the accused guilty of fraud, stating that potential prejudice was present.[51] The court further remarked that

> "[i]t would be monstrous, we think, if because a person's wicked machinations have been defeated, or unsuccessful, on account of the intervention of some third person, or the occurrence of some event beyond his control, or because his misrepresentations were not believed or were not acted upon, that he should escape the penalty of law".[52]

Further authority for Snyman's submission is *R v Seabe*, where the Appellate Division remarked:

> "A person who can barely write and has no idea of spelling presents to a bank a cheque which purports to be drawn by an educated client of the bank. The forgery is so gross that no bank clerk would be deceived. The forger in his ignorance of banking business thought he would get the money. Can we say that because it was probable or reasonably certain that the bank would not cash the cheque there was no potential prejudice to the bank? It has never been suggested to my knowledge that in such a case there is no *crimen falsi*. It seems to me therefore that where there is some risk, though perhaps slight, the element of prejudice necessary to support the *crimen falsi* exists."[53]

Other judgments also support this line of thinking.[54] In *R v Dyonta* the Appellate Division observed that

> "[i]f the representation is one which in the ordinary course is capable of deceiving a person, and thus enabling the accused to achieve his object, the fact that the person to whom the misrepresentation is made has knowledge or a special state of mind which effectively protects him from all danger or prejudice does not entitle the accused to say that the false representation was not calculated to prejudice".[55]

On a similar basis it may be contended that where the representation is one which in the ordinary course is capable of circumventing computer security measures or capable of penetrating a computer system, thus enabling the accused to achieve his object, the fact that the person to whom the misrepresentation is made has knowledge or special software or equipment which effectively protects him from all danger or prejudice does not entitle the accused to say that the false representation was not calculated to prejudice.

With regard to the intent to defraud, numerous courts have stated that the "words 'intent to defraud' must be taken, not in the ordinary narrow sense, but in a wide sense".[56] It can be argued that the hacker intended the computer user to be deceived, by assuming that he was an authorised user or that he had authorised

---

50 1902 NLR 76.
51 81.
52 It should be borne in mind that until 1956 many South African courts did not recognise the offence of attempted fraud.
53 32.
54 See *R v Butler* 1947 2 SA 935 (C) 937; *Kruse* 534; *R v Dyonta* 1935 AD 52 57; *R v Nay* 1934 TPD 52 54; *R v Yenson* 1933 TPD 510 513; *R v Armstrong* 1917 TPD 145 150; *Jolosa* 698.
55 57.
56 *De Vos* 150. See also *Jones* 352–353.

access to the computer system, and that his (the computer user's) action should be affected by the deception.[57]

It is submitted that where the hacker attempts to penetrate the computer system, he has the intention to prejudice seeing that he knows and/or foresees that if he succeeds he will infringe the computer user's right to privacy and depending on the hacker's intention, he further knows and/or foresees that if he copies, modifies or deletes digital files, he will cause prejudice to the computer user, for instance by exposing the computer user to negative media publicity, should this be discovered. The courts (including the Appellate Division) have noted that

> "if a misrepresentation which is capable of deceiving is made wilfully and the person making it intends to deceive the person to whom it is made, that is sufficient to prove the intention to defraud where the misrepresentation is one which causes actual prejudice or is calculated to prejudice".[58]

Therefore, it is submitted that an unsuccessful hacking attempt constitutes fraud.

Even if it were to be argued that an intentional but unsuccessful hacking attempt does not constitute fraud, it is submitted that the accused is guilty of attempted fraud.[59] De Wet and Swanepoel submit that "[a]s die man wat optree met die opset om 'n ander deur misleiding te beweeg om tot sy nadeel te handel nie daarin slaag nie, maak hy hom skuldig aan poging tot bedrog".[60] This submission is also supported by local judgments.[61]

Therefore, it is submitted that the following instances constitute attempted fraud: (a) Where a *hacker* (who made up his mind to hack into the computer system) fails to gain access to the system, after he did everything he could to penetrate the targeted computer's security system and (b) where his conduct constitutes, at least, the commencement of the commencement of the offence.[62]

3227 Does a denial-of-service attack constitute fraud?

Three elements of fraud, namely misrepresentation, prejudice and intent to prejudice, are relevant to this question.

It is submitted that where A launches a denial-of-service attack upon B's computer server, A misrepresents (by *spoofing* the replying address) that he honestly wants to make a connection with B's computer in order for their computers to communicate. A also misrepresents that the address which his computer furnishes to B's computer is his (A's) actual Internet address.

---

57 See *Heyne* 625B–C where the Appellate Division stated: "It is clear that those who were responsible for the wilfully false entries and deliberate omissions from the books intended that the inspecting members of the police should be deceived and that their action should be affected by the deception."

58 *R v Henkes* 1943 AD 143 161. See also *Isaacs* 191D–E.

59 The offence of attempted fraud was recognised by the Appellate Division in *Heyne* 622D–E.

60 *Strafreg* (1985) 404.

61 See *Isaacs* 189D–E.

62 The authors of *LAWSA* para 332 state that where a deliberate fraud was made but no prejudice (actual or potential) resulted, such conduct constitutes attempted fraud. Likewise, Hunt and Milton *South African criminal law and procedure* (1990) 778 aver that the following two instances, *inter alia*, constitute attempted fraud: (a) "Where the misrepresentation is communicated, but it causes no actual prejudice, and because it is so patently ridiculous it is not such as could reasonably harm anyone and there is therefore no potential prejudice either"; and (b) "[w]here for some other reason the misrepresentation, though communicated, contains a risk of prejudice which is 'too remote or fanciful'."

Furthermore, a denial-of-service attack normally results in a computer server being rendered inaccessible or inoperable, which, in turn, leads to a loss of income, communication, business reputation, etc. Where A fails to launch a denial-of-service attack successfully, his conduct entails potential prejudice. Finally, it is submitted that A has the intent to prejudice in that it is his intention to bring A's computer server down. Stated differently, it is his intention to render it inaccessible or inoperable. Therefore, it is submitted that where a cyber-abuser launches a denial-of-service attack on A's computer system, he is guilty of the offence of fraud.

Where A penetrates B's computer and uses it as part of a distributed denial-of-service attack on X's computer, A's conduct constitutes a risk of prosecution for B in that it may appear to the investigating authorities that B launched a denial-of-service attack on X.

3 2 2 8 Does a virus hoax constitute fraud or attempted fraud?

As explained earlier, a virus hoax entails instances where A sends B an e-mail message stating that a new virus was discovered and that the latter must forward this message to everyone he knows. These false warnings pose the risk that too many Internet users might commence e-mailing each other resulting in e-mail servers (either those of employers or Internet Service Providers) being overwhelmed with e-mail messages and consequently either forces system administrators to shut down these servers or causes these servers to crash before system administrators can do anything.

Without repeating the general principles, it is submitted that such conduct constitutes fraud in that:

(a) A makes a misrepresentation: The e-mail message is a perversion of the truth.

(b) A has the necessary intention: *Dolus indeterminatus* is present in that he intentionally sends these false warnings and does not care whose computers will be rendered inoperable.[63]

(c) His conduct is unlawful: The convictions of the community clearly stipulate that these acts are reprehensible in that they can cause extensive financial loss to any Internet connected business, especially businesses that are Internet or e-mail dependent.

(d) Where A is prosecuted before his false warnings had any negative effect on the Internet community, potential prejudice is present in that the virus hoax had the potential to cause financial loss as well as the potential that third parties had to expend time and labour to repair their systems. Where A is prosecuted after his hoax had already caused financial losses and inconvenience, actual prejudice is present.

3 3 Malicious injury to property

Next, the elements of the offence of malicious injury to property are briefly set out. Thereafter these principles are applied to various cyber-abuse instances in order to determine whether they constitute the aforementioned offence.

---

63 Snyman 198 describes *dolus indeterminatus* as follows: "This form of intent is present where someone does not direct his act against a particular person but at anybody who may be affected by his act; the identity of his victims are of no importance to him."

The South African Law Commission was of the opinion that gaining access to a computer without authorisation and modifying information stored on that computer does not constitute malicious injury to property in that the law requires the damaged property to be corporeal.[64] They further maintained that it is uncertain how the concept of "damage", in relation to computer data and software applications, would be interpreted by our courts.[65] Some South African commentators are of the same opinion.[66]

3.3.1 General principles

The traditional definition of malicious injury to property is the unlawful and intentional damaging of property belonging to another.[67] Local courts created a specific exception to this definition, namely that A can be found guilty of malicious injury to property where he sets fire to his own insured property in order to claim its value from the insurance company. This aspect is discussed below.

Five elements have to be present in order for conduct to constitute this offence, namely damage, unlawfulness, causation, intent and property.[68] These elements are now discussed separately:

(a) Damage. Seeing that in the case of computer-related crimes no physical property is damaged, it has to be determined whether the law recognises other forms of "harm" or prejudice as sufficient "damage" for this offence. In *R v Bowden*[69] the accused painted two statues. The court, dealing with the question whether such conduct constitutes damage to property, noted that:

> "Dit is egter wenslik dat daar êrens 'n lyn getrek moet word in verband met die beskadiging van 'n saak. Word 'n saak permanent geskend dan is daar beskadiging as die saak van enige waarde is vir die eienaar. Word 'n saak geskend maar op so 'n manier dat dit herstel kan word en die herstelling lewer koste of moeite vir die eienaar dan is daar ook beskadiging. As die saak self geen waarde het nie of die skade wat berokken word is onbenullig behoort die beskadiging nie as 'n misdaad te geld nie."[70]

Snyman correctly notes that "[d]aar sal gewoonlik aangeneem word dat daar beskadiging is as daar op so 'n manier met die saak gepeuter is dat dit die eienaar geld, arbeid of moeite kos om dit weer te herstel tot sy oorspronklike vorm".[71] For this reason, Burchell and Milton maintain that letting out the air of A's tyres constitutes malicious injury to property in that such conduct interferes with A's use of the property, albeit temporarily.[72] Finally,

---

64 See *Discussion paper 99*: "Computer-related crime: preliminary proposals for reform in respect of unauthorised access to computers, unauthorised modification of computer data and software applications and related procedural aspects" 6.

65 7.

66 Van der Merwe *Computers and the law* (2000) 193; *LAWSA* para 343.

67 *R v Marhanya* 1924 AD 11 12.

68 See *S v Thompson and Strydom* 1964 1 PH H4 (N) 13; *R v Witbooi Motaung* 1954 2 PH H 116 (O); *R v Ncetendaba* 1952 2 SA 647 (SR) 651B; *R v Maruba* 1942 OPD 51 55; *R v Malamu Nkulupaan* 1918 TPD 424 428.

69 1957 3 SA 148 (T).

70 150F–H.

71 Snyman 552. See also *LAWSA* para 344.

72 Burchell and Milton *Principles of criminal law* (2000) 595.

De Wet and Swanepoel observe that "[a]an vernietiging moet mens gelyk stel die wegdoen van 'n saak op so 'n wyse dat dit vir alle praktiese doeleindes nie teruggevind kan word nie".[73] Hunt, in turn, attaches the following meaning to "damage".

"Subject then to the *de minimis* principle, there is damage where X meddles with the property in such a way that it is destroyed or lost or permanently damaged, or damaged with the result that it reasonably requires repair, whether this costs the owner money or labour, or in such a way that its *use is permanently or temporarily interfered with*."[74]

(b) Unlawfulness. A's conduct in causing damage to B's property must be unlawful according to the *boni mores*.

(c) Causation. There must be a causal connection between the damage and the conduct.

(d) Intent. Malice is not required by our courts, even though the offence is known as "malicious injury to property".[75] Mere intent (*opset*) is required[76] and thus *dolus eventualis* as well as *dolus indirectus* will suffice.[77] It is submitted that *dolus indeterminatus* also suffices for the purpose of this offence: "X hoef nie die opset te hê om die een of ander bepaalde persoon te benadeel nie. In baie gevalle van saakbeskadiging weet X trouens nie eers wie die eienaar is nie."[78]

South African courts have invariably required an intention to injure (either the owner or property of the owner) as an essential element of the offence of malicious injury to property.[79] In *R v Maruba* the court noted that "it is not necessary for the Crown to establish the existence of a specific intention to injure the owner: when proof is provided that an accused injured the property of a person, it will be presumed that he intended to injure the owner".[80]

(e) Property. All South African commentators maintain that the object of this offence must be corporeal.[81] The following observations have to be made here: (i) It should be kept in mind that the offence of malicious injury to property did not exist in our common law and that it was created by the Cape Provincial courts.[82] (ii) There exists an exception to the general definition stated above, namely that where someone else has a substantial interest in A's property (such as an insurance company) and A destroys it in

73 De Wet and Swanepoel 288.

74 Hunt "The 'damage' element in malicious injury to property" 1967 *SALJ* 144. My emphasis.

75 *S v Mnyandu* 1973 4 SA 603 (N) 605H.

76 *Mashanga* 12.

77 See *S v Kgware* 1977 2 SA 454 (O) 455E–F; *R v Neuba* 1968 2 SA 18 (R) 19D; *R v Shelembe* 1955 4 SA 410 (N) 411E–F; *R v Ncetendaba supra* 651H.

78 Snyman 553. See also *LAWSA* para 346.

79 See *Mnyandu* 606A; *R v Nkomozombanzo* 1959 1 SA 746 (SR) 764G; *Shelembe* 411D–E; *Ncetendaba* 652B; *R v Maritz* 1944 EDL 101 103; *Kohrs v R* 1940 NPD 11 14; *Malamu Nkalapoan* 425 426; *R v Gordon* 1916 CPD 69 70; *R v Laubscher* 1913 CPD 123 126; *Bruyns v R* 1901 NLR 75 78; *R v Kumana* 1900 EDC 167 168.

80 55. See further *Mashanga* 12; *Malamu Nkalapoan* 428.

81 Burchell and Milton 595; Snyman 551; *LAWSA* para 343; Hunt and Milton 821; De Wet and Swanepoel 289.

82 Burchell and Milton 593; Snyman 550–551; *LAWSA* para 342; De Wet and Swanepoel 286–287. See also *S v Solomon* 1973 4 SA 644 (K) 647H; *Maruba* 54–55.

order to claim money from the insurance company, such conduct not only constitutes fraud but also malicious injury to property.[83] Therefore it seems that "property" includes not only the physical property but also rights that other people have in such property. This submission is confirmed by the following judgments:

- In *R v Mavros* the applicant set his own store on fire with the intent to defraud the insurance company of the money for which he had insured the said store. The accused was charged and found guilty of arson. It should be borne in mind that arson is a *specie* of the offence of malicious injury to property. The Appellate Division maintained that arson is committed by "a man who sets fire to his own house wrongfully, maliciously and with the intent to injure or defraud another person".[84]
- In *Kohrs v R* the accused set four huts on fire. The court stated that "the term 'property' seems to me capable of covering physical objects *as well as rights of all kinds in and to physical objects*, as well as any goods which may reasonably be believed to be in that structure".[85]
- In *S v Mtetwa*[86] the accused killed two cattle belonging to the complainant. The court noted that "in regard to the crime of malicious injury to property it is not necessary that the complainant should be the full and unencumbered owner of the property injured. What is required is that the intentional and unlawful act be an *injury to the rights of another person in and to that property*. Just as a person may be guilty of theft of property of which he is owner (for example, of pledged property belonging to him) so too he may be guilty of malicious injury to property of which he is, in law, the owner but in which other persons have rights."[87]
- In *S v Mnyandu* the court maintained that "'[m]alice' beteken nie wrok of kwaadgesindheid teenoor die eienaar van die beskadigde eiendom of iemand wat 'n *wesenlike belang* daarin het nie".[88]

Consequently, in the light of these judgments, it is submitted that the South African courts have expanded the term "property" to include "substantial interests" as well as "rights in such property", for the purposes of malicious injury to property.[89]

3 3 2 Malicious injury to property over the Internet

The question arises whether the offence of malicious injury to property can be committed with regard to electronic data or content. The following two examples of computer-related abuses serve as points of departure:

(a) A hacks into B's computer and deletes a file or files, corrupts such data or causes a hard drive to be inaccessible by formatting it;

(b) A releases a virus onto the Internet that does the above-mentioned. A knew that the virus had such capabilities.

---

83 See *R v Mavros* 1921 AD 19 below.
84 23.
85 14–15. My emphasis.
86 1963 3 SA 445 (N).
87 449D–F. My emphasis.
88 605H–606A. My emphasis.
89 *Mnyandu* 606A.

As in the case of fraud and theft, such conduct is clearly against the *boni mores* and therefore unlawful. Furthermore, it is assumed that the state can prove that the hacker or virus programme caused such damage. Accordingly, only three elements need to be examined here, namely intent to injure the owner or the property of the owner, damage, and property.

3 3 2 1 Intent to injure the owner or the property of the owner

It is clear that where a hacker intentionally deletes files on a computer he has the intention to injure the owner in that such data will be lost (forever, if the proprietor does not have any back-ups of the information). The same line of reasoning applies where a hacker intentionally causes files to be corrupted, as well as where he formats a hard drive or renders such hard drive permanently inaccessible. By formatting the hard drive, the hacker intends to delete all the files saved on the hard disk. Where the hacker renders a hard drive temporarily inaccessible or inoperable, he has the intent to injure the owner of the computer in that it will take the latter time as well as labour to repair the computer. Where the computer owner uses third parties (such as computer experts) to repair the computer or operating system of the computer or to recover electronic content or some of the content, he suffers financial prejudice. The owner is also prejudiced in his use of the computer system.

Where a virus released onto the Internet causes such damage, the virus programmer definitely had *dolus indeterminatus* in that he released such a dangerous computer programme onto the Internet and did not care whose computers would be rendered inoperable or whose data would be deleted or corrupted.

3 3 2 2 Damage

Where a hacker or a virus programme deletes a file (or even a part of a file) such conduct constitutes damage in that it will take the owner considerable time to recompile the information contained in the original document. The question that arises is what happens where the proprietor made back-up copies. It is submitted that normally the information contained in back-ups will, at least, be a few hours or days old and thus new information is lost. Where up-to-date back-up copies exist, it is submitted that an electronic file (incorporeal property) was still damaged (destroyed) and it will be of no avail for the accused to say that the victim did not suffer loss because he possessed up-to-date back-up copies.

Furthermore, it is submitted that where a hacker or a virus causes a hard drive to be inaccessible, the hacker not only "damages" the electronic data previously stored on the disk, but also damages the disk in that it will take the complainant considerable time to reload all the computer programmes onto the disk in order for the computer to function properly.

Finally, in all these instances the hacker substantially interferes with the use of the property, namely either the electronic file or the hard disk. He either renders the specific data or the entire computer unusable.

3 3 2 3 Property

The question arises whether the property damaged must be corporeal in nature. There are three possible arguments in favour of the view that incorporeal data and content will suffice for his particular requirement:

(a) As indicated above, the courts have repeatedly referred to the rights or interests that people have in corporeal objects. In the case of computer-related crimes, the corporeal object is the hard drive. It is submitted that where a hacker or a malicious computer programme deletes files or corrupts them, he or the programme "destroys" the owner's rights/interests that he enjoys in regard to this hard drive. As mentioned earlier, the owner has an immaterial property right with respect to the electronic content (files) stored on his hard drive. Therefore, although the deletion of the files does not physically damage the hard drive, such deletion does in fact infringe (actually destroys) the owner's immaterial property rights.

Of course, where the hacker or a malicious programme causes the entire hard drive to be formatted or renders it inaccessible, such conduct damages the hard drive as indicated above and therefore physical property is damaged.

(b) The second argument is that the offence of malicious injury to property should develop in an identical way as the offence of theft did. According to Roman law, as well as Roman-Dutch and early South African law, only physical objects (property) could form the subject of theft. New questions of law arose, namely whether money in the form of credit as well as shares, as incorporeal property, could form the object of theft. The courts extended the meaning of "property" to include not only corporeal property but also incorporeal property. In fact, it will be remembered that the courts stated that a mere false entry in an accounting book's credit side constitutes theft.

The same line of reasoning can be followed in the case of malicious injury to property: The meaning of the word "property" should be extended to include incorporeal property embodied in electronic files: By deleting or corrupting data the hacker destroys the electronic content, constituting incorporeal property, and this amounts to what can be called "constructive malicious injury to property". It will be up to the courts to decide what type of information or electronic content can form the object of "constructive malicious injury to property". Hunt and Milton correctly point out that the "property" damaged need not be of commercial value and likewise need not be diminished in commercial value. Explained differently, the conduct need not result in financial loss.[90]

(c) A third possible argument which was upheld by the UK Court of Appeal in *R v Whiteley*[91] is that where information (data) stored on a hard drive is deleted or corrupted, tangible property is damaged:

> "What the [Criminal Damage Act of 1971] requires to be proved is that tangible property has been damaged, not necessarily that the damage itself should be tangible. There can be no doubt that the magnetic particles upon the metal discs were a part of the discs and if the appellant was proved to have intentionally and without lawful excuse altered the particles in such a way as to cause an impairment of the value or usefulness of the disc to the owner, there would be damage within the meaning of section 1. The fact that the alteration could only be perceived by operating the computer did not make the alterations any the less real, or the damage, if the alteration amounted to damage, any the less within the ambit of the Act . . . Any alteration to the physical nature of the property concerned may amount to damage within the meaning of the section. Whether it does so or not will

90 Hunt and Milton 824.

91 1991 93 Cr App R 25. A copy of this judgment can be downloaded from www.austlii.edu.au/au/other/crime/Whiteley.html.

> depend upon the effect that the alteration has had upon the legitimate operator (who for convenience may be referred to as the owner). If the hacker's actions do not go beyond, for example, mere tinkering with an otherwise 'empty' disc, no damage would be established. Where, on the other hand, the interference with the disc amounts to an impairment of the value or usefulness of the disc to the owner, then the necessary damage is established."

The same court confirmed the *dicta* of Auld J in *Morphitis* v *Salmon*[92] where he maintained that "damage should be interpreted so as to include not only permanent or temporary physical harm, but also permanent or temporary, impairment of value or usefulness".[93]

This line of reasoning is also followed in the USA. The facts of *American Guarantee & Liability Insurance v Ingram Micro Inc*[94] were as follows: American Guarantee (the applicant) insured the computers of Ingram Micro (the respondent) in terms of its "Primary-All-Risk Policy". This policy insured all respondent's "[r]eal, and personal property, business income and operations in the world" against "[a]ll risks of direct physical loss or damage from any cause, howsoever or wheresoever occurring, including general average, salvage charges or other charges, expenses and freight". As a result of a power outage, respondent's computer systems were rendered inoperable. Specifically, the main frame computers lost all of the programming information that had been stored in their "random access memory". Respondent's employees had to reload the lost programming information, which took about one and a half hours. It took these employees a further six and a half hours to restore the computers, and their connections to other computers around the world, to their normal functioning. It follows that respondent could only conduct business as normal after eight hours.

Applicant refused to pay the claimed insurance, averring that respondent's computers were not physically damaged "because their capability to perform their intended functions remained intact. The power outage did not adversely affect the equipment's inherent capability to accept and process data and configuration settings when they were subsequently reentered into the computer system". The respondent, in turn, argued that "physical damage" must be interpreted more generously to include "loss of use and functionality". The court sided with the plaintiff and held:

> "At a time when computer technology dominates our professional as well as personal lives, the Court must side with Ingram's broader definition of 'physical damage.' The Court finds that 'physical damage' is not restricted to the physical destruction or harm of computer circuitry but includes loss of access, loss of use, and loss of functionality . . . Lawmakers around the country have determined that when a computer's data is unavailable, there is damage; when a computer's services are interrupted, there is damage; and when a computer's software or network is altered, there is damage. Restricting the Policy's language to that proposed by American would be archaic . . . In this case, Ingram does allege property damage – that as a result of the power outage, Ingram's computer system and world-wide computer network physically lost the programming information

92 1990 Crim LR 48.

93 Unfortunately this case was not locally available, so I had to rely on Akdeniz "Section 3 of the Computer Misuse Act 1990: an Antidote for Computer Viruses!" 1996 http://webjcli.ncl.ac.uk/1996/issue3/akdeniz3.html.

94 2000 WL 726789 (D Ariz 2000). A copy of this judgment can be downloaded from www.2001law.com/article_445.htm.

well as hard drive space) to be consumed and eventually the computer stops functioning. Such conduct clearly constitutes malicious injury to property in that:

(a) The computer programme substantially interferes with the use of the computer. Normally the computer owner (or his system administrator) has to spend time and money to remove the malicious computer programme and to repair the computer system. Therefore damage is present.

(b) Unlawfulness as well as causation is present.

(c) *Dolus indeterminatus* is present in that the programme creator knew that his programme had this potential, but did not care who suffered the consequent prejudice.

(d) The computer system (as corporeal property) is damaged: It is rendered inoperable.

3 3 5 Denial-of-service attacks and e-mail bomb attacks

Bearing in mind the general principles of malicious injury to property, it is submitted that both denial-of-service attacks and e-mail bomb attacks constitute malicious injury to property in that property, in this case the computer which includes its operating system (such as MS Windows), is damaged:

(a) It will either cost the owner money or labour and effort to restore the computer to a working condition; and

(b) It interferes with the use of the computer to such an extent that the computer owner cannot enjoy his subjective rights; and

(c) The hacker clearly has *dolus directus* in that his actions are specifically directed against the targeted computer user. Of necessity, the elements of unlawfulness and causation are present.

3 3 6 Defacement of a web page by a hacker or computer programme

Next the question whether the defacement of a web page, either by a hacker himself or by using a malicious computer programme, constitutes malicious injury to property, is addressed.

Defacement of a web page can occur in one of two ways: (a) When a hacker gains access to a web site and defaces a particular web page; or (b) when a person employs an insidious computer programme to infect the computer hosting a web site and the programme defaces a web page. The defacement of a web page can refer to various aspects of which the following are mere examples:

- The wording of an online news report can be changed (for example, to read that Bill Gates hacked into NASA's computer system) or the prices of an online inventory can be modified (for example, R2.99 instead of R299); or
- a message can be displayed on the web page, in addition to the normal contents of this particular page (for example, stating that "Mafiaboy was here" or that "your network security sucks"); or
- the entire web page content is deleted and replaced with the hacker's web page, which, in turn, can include pornographic material, defamatory statements or irrelevant content.

It is submitted that where a hacker defaces a web page by deleting the content of the web page and then replacing it with his own content, such conduct constitutes malicious injury to property in that he infringes the web page owner's immaterial property rights: He "destroyed" the owner's incorporeal property.

> and custom configurations necessary for them to function. Ingram's mainframes were 'physically damaged' for one and one half hours.' It wasn't until Ingram employees manually reloaded the lost programming information that the mainframes were 'repaired.' [The computer] was 'physically damaged' for eight hours. Ingram employees 'repaired' [the computers] by physically bypassing a malfunctioning matrix switch. Until this restorative work was conducted, Ingram's mainframes and [computers] were inoperable."

In *Retail Systems Inc v CAN Insurance Cos*[95] the facts were that the appellant lost A's computer tape containing valuable information. Respondent insured the appellant against damage claims resulting from "Personal Injury or Property Damage to which this insurance applies". The policy continued to define property damage as "physical injury or destruction of tangible property". The respondent contended that only the loss of the computer tape was covered by the insurance policy and not the data stored on the tape. The question of law was whether the computer tape and the data stored on it were tangible property under the insurance policy. The court answered this question in the affirmative by noting that

> "[t]he data on the tape was of permanent value and was integrated completely with the physical property of the tape. Like a motion picture, where the information and the celluloid medium are integrated, so too were the tape and data integrated at the moment the tape was lost".[96]

Therefore, it is submitted that where a hacker or the creator of a malicious computer programme causes information to be deleted or corrupted or renders a hard drive inaccessible, such conduct justifies a conviction of the offence of malicious injury to property.

3 3 3 Modification of digital content and malicious injury to property

It is submitted that where a hacker modifies the electronic content stored on a computer or uses a malicious computer programme to modify electronic files, such conduct constitutes malicious injury to property in that:

(a) Damage will be present where, due to the modification, the owner has to spend time, money and labour to repair the file or to restore it to its original form. Where an electronic file is modified it interferes with the owner's use of these files. Furthermore, where the file is rendered unusable due to the modification, the file is for all purposes permanently damaged.

(b) Such conduct is clearly unlawful.

(c) The hacker or the computer programmer cause such damage or prejudice.

(d) Intent is present in that the hacker has *dolus directus* and the computer programmer (who created the virus) has *dolus indeterminatus*.

(e) They cause damage to electronic content and thus incorporeal (immaterial) property. They also infringed the owner's legal interest he enjoys in the immaterial content.

3 3 4 Bacteria and malicious injury to property

As noted earlier, bacteria are computer programmes programmed to replicate *ad infinitum* within a computer system. This causes system resources (memory as

95 469 NW 2d 735 (Minn App 1991).
96 737.

Furthermore it will normally cost the owner time and labour to rebuild the web page or to recompile the information displayed on the previous web page.

Where text or pictures are added to a web page, such conduct is tantamount to graffiti. Only where the removal of the text or content added to the web page costs the owner labour, time and/or money to restore the page to its original condition, will such conduct constitute malicious injury to property.[97]

The *de minimis non curat lex* rule should also be kept in mind. Whether this rule applies to a given scenario depends upon the facts of the particular scenario. The general criterion seems to be: Was the damage done, if any, of such a trifling nature that the matter should never have come to court?[98]

8.16

3 3 7 *Attempt to commit malicious injury to property*

Under this heading it is ascertained whether someone can be found guilty of an attempt to commit malicious injury to property where he intentionally releases sinister computer programmes but such programmes are either defective (and cannot cause any prejudice) or the programmes are discovered before they can cause any prejudice. Therefore, no actual prejudice is caused.

8.17

3 3 7 1 Virus discovered prior to causing prejudice

Where A intentionally sends a malicious computer programme as an e-mail attachment to B, intending to cause the latter either inconvenience or financial loss, but B discovers in time that the attachment contains a malicious programme and consequently suffers no prejudice, the question of law arises whether A can be prosecuted for attempted malicious injury to property. It is assumed that if the computer programme was not discovered and subsequently removed by B, it would either have deleted, modified or corrupted information stored on B's hard drive or would have rendered B's computer inoperable or inaccessible.

8.18

A court will find an accused guilty of an attempt to commit a crime where (a) the accused had the intent to commit the particular crime; and (b) an overt act (*actus reus*) is present.[99] With regard to the various types of "attempts" that exist in our law, the Appellate Division maintained in *R v Schoombie*[100] that

> "[a]ttempts seem to fall naturally in two classes: (a) Those in which the wrongdoer, intending to commit a crime, has done everything which he set out to do but has failed in his purpose either through lack of skill, or of foresight, or through the existence of some unexpected obstacle, or otherwise, (b) those in which the wrongdoer has not completed all that he set out to do, because the completion of his unlawful acts has been prevented by the intervention of some outside agency".[101]

8.19

The postulated example can be compared with the facts in *S v Laurence*.[102] The accused dispatched an envelope (containing an article, which, if published in South Africa, would have rendered the accused liable in terms of the Suppression of Communism Act) to A in London requesting him to forward the article to B, a

97 See *Bowden* 150F–G.
98 *Mbala v S* 1969 1 PH H44; *R v Dane* 1957 2 SA 472 (N) 473B–C.
99 *S v Du Plessis* 1981 3 SA 382 (A) 401C.
100 1945 AD 541.
101 547.
102 1975 4 SA 825 (A).

publisher of a newspaper which would in the normal course of events have been circulated in South Africa. The envelope was intercepted and the accused was subsequently charged with attempt to contravene this Act. The Appellate Division simply stated that

> "he did everything which he set out to do; he could do no more and dropped out of the picture after he had completed his self-imposed task. On a realistic, common sense view the role played by the appellant clearly constituted a completed attempt".[103]

8.17

Therefore, it may safely be stated that in our given example the frustration of the completion of the offence was beyond A's control. There was no further step that the accused could haven taken towards the consummation of the offence.[104] The accused also had the necessary intent to commit the crime, namely either *dolus directus* or *dolus eventualis*. Therefore, it is submitted that he is guilty of attempted malicious injury to property.

3 3 7 2 Target computer not vulnerable to computer programme

The question that arises is: What would the position be if a malicious programme is designed to delete or corrupt specific files, such as files ending with ".gif", and the computer of the complainant contains no such files? Even if the complainant fails to detect the malicious programme he will not suffer prejudice. The question therefore is whether such conduct constitutes attempted malicious injury to property.

8.20

It is clear that the accused did everything he could to commit the crime. It follows that this is a completed attempt but the question remains whether it is possible to hold an accused liable for an attempt to commit an offence where the offence that he attempted to commit was impossible.

In *R v Davies*[105] the Appellate Division dealt with an attempt to commit the impossible. The accused (a doctor) had attempted to conduct an illegal abortion, but unknown to him the *foetus* was already dead. The court maintained that

> "it seems that on principle the fact that an accused's criminal purpose cannot be achieved, whether because the means are, in the existing or in all conceivable circumstances, inadequate, or because the object is, in the existing or in all conceivable circumstances, unattainable, does not prevent his endeavour from amounting to an attempt".[106]

8.20

Furthermore, the court noted that

> "it would obviously be reasonable to treat as attempts all cases where an endeavour, going beyond preparation, has been made to procure an abortion, *whether or not the woman was pregnant, the foetus alive or the means capable of achieving the purpose aimed at*".[107]

Therefore, it is submitted that in the given scenario either the means the accused used was inadequate (he should have used another computer programme to delete files) or the object at which he directed his acts was unattainable (he could not cause prejudice to B in that his hard drive, the object, contained no such

---

103 827H–828A. See also *R v Lionda* 1944 AD 348 355–357.
104 See *S v Mlambo* 1986 4 SA 34 (E) 41G–H 41J–42B.
105 1956 3 SA 52 (A).
106 64A–B.
107 64H. My emphasis.

files). He also has the necessary intent to commit the crime. Therefore, it is submitted that he is guilty of attempted malicious injury to property.

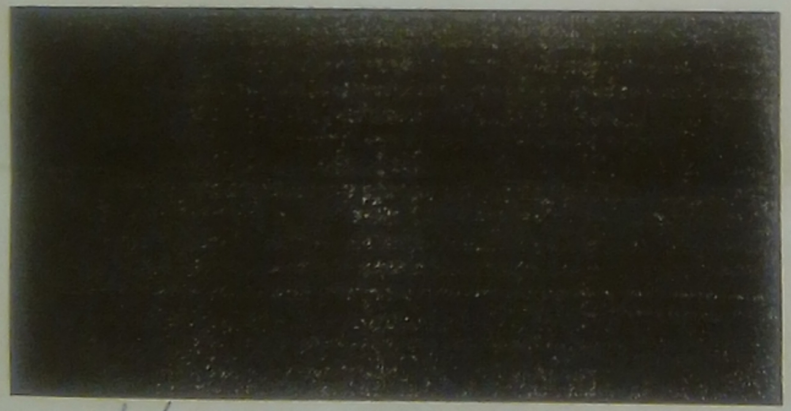
3 3 7 3 Defective malicious programmes

Another question that can be asked is what the legal position is where A, a computer programmer, creates a malicious computer programme, releases it onto the Internet to wreak havoc, but it turns out that the programme is defective and cannot cause prejudice to anyone. B contracts the virus.

It is submitted that this also constitutes a completed attempt in that A did everything he could to commit the crime, but failed to succeed because the means he used to commit the crime was not capable of committing the crime. He also had the necessary intent to commit the crime. It is submitted that a court will probably hold that *dolus indeterminatus* was present.

(To be continued)

dolus directus
dolus indirectus



dolus eventualus
dolus indeterminatus

the unlawfull